UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

UNITED STATES OF AMERICA,	)	
	)	
v.	)	No. 3:08-CR-175
	)	Judges Phillips/Shirley
CLARK ALAN ROBERTS, and	)	
SEAN EDWARD HOWLEY	)	
	)	
Defendants.	)	

UNITED STATES' OPPOSITION TO
DEFENDANT ROBERTS' MOTION TO SUPPRESS EVIDENCE

The United States of America, by and through James R. Dedrick, United States Attorney for the Eastern District of Tennessee, respectfully submits this response in opposition to the Defendant Roberts' Motion to Suppress Evidence based on the search warrant used to search computers at the premises of Wyko Tire Technology, Inc., Defendant Roberts' place of employment.[1] The motion should be denied on the grounds that the Defendant does not have standing to challenge the warrant and the warrant establishes probable cause to search the computers and seize the contents thereof.

Defendant Roberts lacks standing to challenge the warrant executed at Wyko's business premises authorizing the seizure of Wyko's business records. He has not established an expectation of privacy in Wyko's business records. Without such an expectation of privacy he

[1]/ The warrant authorized the search and seizure of other items, including documents. The Defendant's motion does not complain about the search and seizure of non-computer items of evidence.

has no standing. Defendant's citation of *United States v. Mohney*, 949 F.2d 1347 (6th Cir. 1991) to support his claim of standing is clearly misplaced. In *Mohney*, the Court found that the individual defendant did not have standing to challenge the search warrant executed at a corporation's premises. The "rights assured by the Fourth Amendment are personal rights, [which] ... may be enforced by exclusion of evidence only at the instance of one whose own protection was infringed by the search and seizure." *Simmons v. United States*, 390 U.S. 377, 389, 88 S.Ct. 967, 974, 19 L.Ed.2d 1247 (1968), *quoted in Rakas v. Illinois*, 439 U.S. 128, 138, 99 S.Ct. 421, 427, 58 L.Ed.2d 387 (1978). While the Mohney court did recognize that "in some circumstances, an officer of a corporation may be a 'person aggrieved' by a corporate search and seizure and thus have standing to challenge the search," 949 F2d at 1403, it, nevertheless held, [w]here the documents seized were normal corporate records not personally prepared by the defendant and not taken from his personal office, desk, or files, in a search that was not directed at him personally, the defendant cannot challenge a search as he would not have a reasonable expectation of privacy in such materials. *Id*., *citing United States v. Britt*, 508 F.2d 1052, 1055 (5th Cir.), *cert. denied*, 423 U.S. 825, 96 S.Ct. 40, 46 L.Ed.2d 42 (1975). As the Second Circuit so succinctly held, "When a man chooses to avail himself of the privilege of doing business as a corporation, even though he is its sole shareholder, he may not vicariously take on the privilege of the corporation under the Fourth Amendment; documents which he could have protected from seizure, if they had been his own, may be used against him, no matter how they were obtained from the corporation." *Lagow v. United States*, 159 F.2d 245, 246 (2d Cir. 1946). Defendant Roberts does not have standing to challenge the seizure of Wyko's records.

Even if Defendant Roberts did have standing, the warrant establishes probable cause. As set forth below, a search warrant was duly reviewed and signed authorizing the search and seizure of Wyko's computers and computer-related documentation. Agents, while executing a search warrant, searched and seized computer servers and computer hard drives belonging to Wyko and located at Wyko's business premises in Greenback, Tennessee. The computer servers and hard drives were seized because they were likely to contain records called for by the warrant. The warrant authorized the seizure, and therefore also authorized agents to search through the seized computer files for those records. The warrant complied with the Fourth Amendment's particularity requirement and comports with precedent from this district and the Sixth Circuit, including *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001).

The defense argument is largely a generalized challenge to the sufficiency of the search warrant to search computers. Similar arguments were recently considered and rejected in a well-considered decision by Judge Greer. *See United States v. Tillotson*, No. 2:08-CR-33, 2008 WL 5140773 (E.D. Tenn. Dec. 2, 2008)). Finally, even assuming arguendo, that the Defendant could establish a particularity violation, he is not entitled to suppression. The Defendant's motion must be denied.

When a search warrant authorizes agents to search a premises and seize things that might be stored on a computer, agents have the authority to seize any computer on the premises that might contain those things and search through that computer off-site. *See Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001). The *Guest* decision supports the issuance of the search warrant in this case. In *Guest*, police executed a warrant that commanded them to search for particular electronic communications. The police took entire computers from the premises and subjected

them to off-site analysis. The Sixth Circuit concluded this procedure did not violate the Fourth Amendment:

> "Although there were presumably communications on the computers that did not relate to the offenses, "[a] search does not become invalid merely because some items not covered by a warrant are seized." *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir.1988). … In the instant cases, when the seizures occurred, defendants were unable to separate relevant files from unrelated files, so they took the computers to be able to sort out the documents off-site. Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files."

Guest, 255 F.3d at 334-35. *Guest* established that the practice of seizing an entire computer (or a copy of it) from a premises and continuing the search of that computer later, off-site, is consistent with the Fourth Amendment. The *Guest* court held this was so even though the seizure of an entire computer necessarily also "seizes" data stored on that computer that is otherwise not called for by the warrant. *Id.* Not surprisingly, every other circuit to consider this question has arrived at the same answer. *See United States v. Giberson*, 527 F.3d 882, 886-87 (9th Cir. 2008) (holding that a warrant that "clearly limited the types of documents and records that were seizable" permitted the seizure of an entire computer); *United States v. Grimmett*, 439 F.3d 1263, 1269 (10th Cir. 2006); *United States v. Campos*, 221 F.3d 1143, 1147 (10th Cir. 2000) (upholding seizure of "computer equipment which may be, or is used to visually depict child pornography"); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (upholding seizure of "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in a child pornography case because "[a]s a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and

seizure reasonably likely to obtain the [sought after] images"); *Davis v. Gracey,* 111 F.3d 1472, 1480 (10th Cir. 1997) ("we can find no legal or practical basis for requiring officers to avoid seizing a computer's contents in order to preserve the legality of the seizure of the computer hardware"); *United States v. Henson,* 848 F.2d 1374, 1382-83 (6th Cir. 1988).

The Defendant contends that the warrant was a prohibited general warrant because "[t]here was no way for an agent executing the warrant to ascertain, from looking at the computer server or individual computer, whether it is something to be seized without conducting a further and more particularized search of the contents of the computer data." Defendant's memorandum at page 4. Defendant cites no authority for this position.

Judge Greer recently rejected essentially the same argument in *United States v. Tillotson,* No. 2:08-CR-33, 2008 WL 5140773 (E.D. Tenn. Dec. 2, 2008). *See* Exhibit 1 (copy of *Tillotson* decision). In that case, a warrant authorized a search for child pornography. The court held:

> "It is the manner of that storage that dictates the scope of search warrants for electronically-stored information. Files on computers containing child pornography likely would not be identified as "My Child Porn;" rather, knowing that pornographic depictions of minors are highly illegal, the owner would be expected to store the data in innocuously-named files. To search for specific data on a computer, such as child pornography, or data concerning child pornography (correspondence, e.g.), it is necessary to search basically every file on the computer."

Tillotson, 2008 WL 5140773 at *4.

Because the warrant authorized the agents to search for particular computer records, it therefore authorized them to look through Wyko's computers for those records. It is black-letter law that agents executing a search warrant may examine the contents of containers if it is "reasonable to expect that the items enumerated in the search warrant could be found therein."

United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008). As the Defendant points out, computers are analogous to containers, and, therefore, "a warrant that describes particular documents authorizes the seizure of a computer where… the searching agents reasonably believed that documents specified in the warrant would be found stored in the computer." *Giberson,* 527 F.3d at 886. What's more, such a "computer search may be as extensive as reasonably required to locate the items described in the warrant." *United States v. Grimmett,* 439 F.3d 1263, 1270 (10th Cir. 2006).

The process of searching through a computer—like the process of searching through a desk drawer, filing cabinet, or bedroom—necessarily requires agents to inspect some items that are not called for by the warrant in the course of looking for those items that are. This is reasonable when done as part of physical searches, *see, e.g., Andresen v. Maryland,* 427 U.S. 463, 482 n.11 (1976) ("it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized"), and is reasonable in computer searches as well, *see Tillotson,* 2008 WL 5140773 at *4 ("it is necessary to search basically every file on the computer").

The Defendant also argues the warrant violated the particularity clause because it failed to specify the places on the hard drive to be searched and a methodology for conducting the search. The Fourth Amendment requires no such limitations on a warrant, and in practice such limitations would be difficult.

In general, "[n]othing in the language of the Constitution or in [the Supreme Court's] decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise

manner in which they are to be executed." *United States v. Grubbs*, 547 U.S. 90, 98 (2006) (*quoting Dalia v. United States*, 441 U.S. 238, 255 (1979)). "It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers." *Dalia*, 441 U.S. at 258.

Several Circuit Courts have applied this rule to computer searches and upheld computer search warrants that included neither a protocol (a list of steps the investigator is required to undertake in examining the computer) nor an explanation for the lack of a protocol. In *United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008), the court upheld a seizure of a computer and a search through it for particularly described records, even though the records were intermingled with other files, without requiring any protocol. The Court held that "[w]hile officers ought to exercise caution… the potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment's reasonableness requirement." *Id.* at 888-89. In *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006), the defendant challenged the search of his computer, arguing, among other things, that the warrant was invalid because "it did not include a search protocol to limit the officer's discretion as to what they could examine when searching the defendant's computer media." *Id.* at 977. The court held that no search protocol was necessary, and that it also was not necessary to explain the absence of a search protocol in the warrant application. *Id.* at 978. The Tenth Circuit emphasized in *United States v. Brooks*, 427 F.3d 1246 (10th Cir. 2005), that while warrants must describe "with particularity the objects of their search," the methodology used to find those objects need not be described: "This court has never required warrants to contain a

particularized computer search strategy." *Id.* at 1251. In *United States v. Khanani,* 502 F.3d 1281, 1290-91 (11th Cir. 2007), the Eleventh Circuit rejected the argument that a warrant should have included a search protocol, pointing in part to the careful steps agents took to ensure compliance with the warrant. *See also United States v. Cartier,* 543 F.3d 442, 447-48 (8th Cir. 2008) ("While we acknowledge that there may be times that a search methodology or strategy may be useful or necessary, we decline to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se"); *United States v. Upham,* 168 F.3d 532, 537 (1st Cir. 1999) ("The warrant process is primarily concerned with identifying *what* may be searched or seized — not how").

Agents already operate under significant constitutional restrictions when they search a hard drive. As with any search, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Dalia,* 441 U.S. at 258; *United States v. Ramirez,* 523 U.S. 65, 71 (1977) ("The general touchstone of reasonableness which governs Fourth Amendment analysis ... governs the method of execution of the warrant."); *Hill,* 459 F.3d at 978 ("reasonableness of the officer's acts both in executing the warrant and in performing a subsequent search of seized materials remains subject to judicial review."). Unreasonable conduct can be remedied after the fact.[2]

---

[2] The Defendant is simply wrong when he argues that a Department of Justice manual agrees that the "best practice" is to "state[] which terms could be searched on the computer and the methodology for searching them." (Mot. at 19). That Manual never argued that the Fourth Amendment required an explanation of search strategy in the affidavit, or recommended that the search strategy be made a condition of the warrant. It recommended including a search strategy as a means of heading off later defense arguments that the search was conducted unreasonably. *See* Computer Crime and Intellectual Property Section, U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 100-01 (2d ed. 2002).

Finally, even if the Defendant had standing and had established a particularity violation, that would not justify suppression. In general, suppression of evidence is a "last resort," *Hudson v. Michigan*, 547 U.S. 586, 591 (2006), appropriate only when law enforcement conduct is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, _ S.Ct. _, No. 07-513, 2009 WL 77886, *7 (U.S. Jan. 14, 2009). Suppression because of an overbroad warrant is particularly disfavored:

> "[I]nfirmity due to overbreadth does not doom the entire warrant; rather, it "requires the suppression of evidence seized pursuant to that part of the warrant ..., but does not require the suppression of anything described in the valid portions of the warrant (or lawfully seized-on plain view grounds, for example-during their execution). *United States v. Brown*, 984 F.2d 1074, 1077 (10th Cir. 1993) (internal quotes and citation omitted)."

United States v. Greene, 250 F.3d 471, 477 (6th Cir. 2001).

Respectfully submitted this 5th day of June, 2009.

JAMES R. DEDRICK
United States Attorney

S/ D. Gregory Weddle
S/ Thomas Dougherty

_____

D. Gregory Weddle
Thomas Dougherty
Assistant U.S. Attorneys
800 Market Street, Suite 211
Knoxville, TN 37902
865-225-1710

CERTIFICATE OF SERVICE

I hereby certify that on June 5, 2009, a copy of the foregoing UNITED STATES' OPPOSITION TO DEFENDANT ROBERTS' MOTION TO SUPPRESS EVIDENCE was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. All other parties will be served by regular U.S. mail. Parties may access this filing through the Court's electronic filing system.

S/ D. Gregory Weddle
S/ Thomas Dougherty

D. Gregory Weddle
Thomas Dougherty
Assistant U.S. Attorneys
800 Market Street, Suite 211
Knoxville, TN 37902
865-225-1710